State of Michigan - (agency name)
Biennial Evaluation of the Internal Control Structure - Application Environment Controls
As of September 30. 2004

Note: Due to the formation of the Department of Information Technology (DIT), many IT related responsibilities that were formally assumed by Agency/Department management has shifted to DIT management. However, Agency management is still the business process/application owners, and therefore, sill hold the responsibility for managing the application and the application environment.

Application Environment Controls do not apply to an individual computer system, but apply to the entire environment in which the Department's/Agency's various computer applications reside. These types of controls differ from application specific controls (which apply to individual applications) and general controls (which apply to statewide or DIT-wide controls). Application environment controls may include controls related to agency management aims and objectives, performing risk assessments of computer applications, installing and accrediting computer systems, service level agreements, obtaining independent assurance, monitoring the IT processes, data storage/retrieval. Ensuring these controls are in place is primarily the responsibility of the business process management/agency management for which the information system was developed. However, the responsibility for some of these controls may cross over into joint responsibility with IT management (DIT management).

(1)	(2)	(3)	(4)				(5)					(6)	(7)
Optimal Internal Controls	COBIT reference	Agency, Division/Office and Staff (non-DIT) responsible for IT process and related controls identify the activity and business owner responsible for each IT process (e.g., agency, division, office and/or staff)	Internal Control Existence (a)				Performance Effectiveness					Description/Comments (this column must be completed) description of controls, activities, formal policies, procedures, and practices that represent internal controls related to the IT process and whether alternative or compensating controls and plans and time frames exist for addressing deficiencies	Monitoring (this column must be completed) description of activities performed to ensure controls in place are working
			Documented	Not Documented	No Control in Place	Not Applicable (b)	Excellent	Very Good	Satisfactory	Ineffective/Inefficient	Not Applicable		
Information Technology Strategic Plan													
Objective: A strategic planning process is undertaken at regular intervals and long-term plans are periodically translated into operational plans, with setting of clear and concrete short-term goals.													
Potential/Likely Risks: There is not a regular review of the strategic plan.													
IT as Part of the Organization's Long- and Short-Range Plan													
Has a strategic IT plan been developed and implemented that addresses the long and short range plans that fulfill the organization's mission and goals?	PO 1.1												
IT Long-Range Plan													
Does the IT planning process include mechanisms to solicit input from relevant internal and external stakeholders impacted by the IT strategic plans?	PO 1.2												
IT Long-Range Planning – Approach and Structure													
Does the IT planning process take risk management results, organizational changes, technological evolution, costs, legal and regulatory requirements into consideration?	PO 1.3												
IT Long-Range Plan Changes													
Is a process in place to modify IT long range plans in a timely and accurate manner?	PO 1.4												
Short-Range Planning for the IT Function													
Are IT short-range plans reassessed periodically and amended as necessary in response to the changing business and IT conditions?	PO 1.5												
Communication of IT Plans													
Have strategic IT long and short-range plans been communicated to business process owners and	PO1.6												

(a) When possible, obtain applicable documentation and/or flowcharts for your future needs/requirements. (b) Please explain in the Description/Comments Column

(1)	(2)	(3)	(4)				(5)					(6)	(7)
Optimal Internal Controls	COBIT reference	Agency, Division/Office and Staff (non-DIT) responsible for IT process and related controls identify the activity and business owner responsible for each IT process (e.g., agency, division, office and/or staff)	Internal Control Existence (a)				Performance Effectiveness					Description/Comments (this column must be completed) description of controls, activities, formal policies, procedures, and practices that represent internal controls related to the IT process and whether alternative or compensating controls and plans and time frames exist for addressing deficiencies	Monitoring (this column must be completed) description of activities performed to ensure controls in place are working
			Documented	Not Documented	No Control in Place	Not Applicable (b)	Excellent	Very Good	Satisfactory	Ineffective/Inefficient	Not Applicable		
other relevant parties across the organization?													
Monitoring and Evaluating of IT Plans													
Has a process been established to capture feedback from business process owners and users?	PO1.7												
Assessment of Existing Systems													
Is there a process in place to assess the existing information system in terms of the degree of business automation, functionality, and stability prior to developing or changing the strategic or long range IT plan?	PO1.8												

Conclusion for this Section (Include All Weaknesses Identified)

Defining the Information Technology Organization and Relationships													
Objective: Determine that the right information technology services are delivered.													
Potential/Likely Risks: The IT organization roles and responsibilities are not defined or communicated or aligned with the business to facilitate the strategy providing for effective direction and adequate control.													
IT Planning or Steering Committee													
Has senior management appointed a planning or steering committee to oversee the IT function and its activities?	PO4.1												
Roles and Responsibilities													
Does the employee have sufficient authority to exercise the roles and responsibilities assigned to them?	PO4.4												
Ownership and Custodianship													
Has management created a structure for formally appointing data owners and custodians?	PO4.7												
Data and System Ownership													
Do all information assets (data and systems) have an appointed owner who makes decisions about classification and access rights?	PO 4.8												
Segregation of Duties													
Has agency management implemented a division of roles and responsibilities that excludes the possibility for a single individual to subvert a critical process?	PO 4.10												
Contracted Staff Policies and Procedures													
Has management implemented policies and	PO 4.14												

(a) When possible, obtain applicable documentation and/or flowcharts for your future needs/requirements.

(b) Please explain in the Description/Comments Column

(1)	(2)	(3)	(4)				(5)					(6)	(7)
Optimal Internal Controls	COBIT reference	Agency, Division/Office and Staff (non-DIT) responsible for IT process and related controls identify the activity and business owner responsible for each IT process (e.g., agency, division, office and/or staff)	Internal Control Existence (a)				Performance Effectiveness					Description/Comments (this column must be completed) description of controls, activities, formal policies, procedures, and practices that represent internal controls related to the IT process and whether alternative or compensating controls and plans and time frames exist for addressing deficiencies	Monitoring (this column must be completed) description of activities performed to ensure controls in place are working
			Documented	Not Documented	No Control in Place	Not Applicable (b)	Excellent	Very Good	Satisfactory	Ineffective/Inefficient	Not Applicable		
procedures for controlling the activities of consultants and other contract personnel to ensure the protection of the information technology assets?													
Relationships													
Has agency and IT management taken the necessary actions to establish and maintain an optimal coordination, communication, and liaison structure between the IT function and others inside and outside the function (e.g., users, security officers, risk managers, suppliers)?	PO 4.15												
Conclusion for this Section (Include All Weaknesses Identified)													
Managing the Information Technology Investment													
Objective: To ensure appropriate funding is available and to control disbursements of the financial resources.													
Potential/Likely Risks: A periodic investment and operational budget is not established and approved by the business.													
Annual IT Operating Budget													
Has a budgeting process been implemented to ensure that an annual IT operating budget is established and approved in line with the agency's long and short range plans?	PO 5.1												
Cost and Benefit Monitoring													
Has management established a cost monitoring process comparing actual to budget?	PO 5.2												
Cost and Benefit Justification													
Is a control in place to guarantee that the delivery of services by the IT function is cost justified?	PO 5.3												
Conclusion for this Section (Include All Weaknesses Identified)													
Communicating Management Aims and Directions													
Objective: To ensure user awareness and understanding of management's plans for the information technology environment.													
Potential/Likely Risks: Policies are not established and communicated to the user community. Standards are not established to translate the strategic options into practical and usable user roles.													
Positive Information Control Environment													
Does agency management ensure that all personnel	PO 6.1												

(a) When possible, obtain applicable documentation and/or flowcharts for your future needs/requirements.

(b) Please explain in the Description/Comments Column

(1)	(2)	(3)	(4)				(5)					(6)	(7)
Optimal Internal Controls	COBIT reference	Agency, Division/Office and Staff (non-DIT) responsible for IT process and related controls identify the activity and business owner responsible for each IT process (e.g., agency, division, office and/or staff)	Internal Control Existence (a)				Performance Effectiveness					Description/Comments (this column must be completed) description of controls, activities, formal policies, procedures, and practices that represent internal controls related to the IT process and whether alternative or compensating controls and plans and time frames exist for addressing deficiencies	Monitoring (this column must be completed) description of activities performed to ensure controls in place are working
			Documented	Not Documented	No Control in Place	Not Applicable (b)	Excellent	Very Good	Satisfactory	Ineffective/Inefficient	Not Applicable		
in the organization have and know their responsibilities in relation to information systems?													
Has agency management created a framework and an awareness program fostering a positive control environment throughout the entire organization by addressing aspects such as integrity, ethical values, competence of people, management philosophy and operating style, accountability, and direction?	PO 6.1												
Management's Responsibility for Policies													
Has agency management assumed full responsibility for formulating, developing, documenting, promulgating, and controlling policies covering general aims and directives?	PO 6.2												
Communication of Organization Policies													
Are organizational policies communicated to and understood by all levels in the organization?	PO 6.3												
Policy Implementation Resources													
Has agency management earmarked appropriate resources for the implementation of its policies?	PO 6.4												
Maintenance of Policies													
Is there a framework and process in place for the periodic review and approval of standards, policies, directives, and procedures?	PO 6.5												
Compliance with Policies, Procedures and Standards													
Are there appropriate procedures in place to determine whether personnel understand the implemented policies and procedures, and that policies and procedures are being followed?	PO 6.6												
Quality Commitment													
Has agency and IT management defined, documented, and maintained quality philosophy, policies, and objectives that are understood and implemented at all levels of the IT function?	PO 6.7												
Security and Internal Control Framework Policy													
Has agency management assumed full responsibility for developing and maintaining a framework policy that establishes the organization's overall approach to security internal control?	PO 6.8												
Intellectual Property Rights													
Is there a written policy on intellectual property rights	PO 6.9												

(a) When possible, obtain applicable documentation and/or flowcharts for your future needs/requirements. (b) Please explain in the Description/Comments Column

(1)	(2)	(3)	(4)				(5)					(6)	(7)
Optimal Internal Controls	COBIT reference	Agency, Division/Office and Staff (non-DIT) responsible for IT process and related controls identify the activity and business owner responsible for each IT process (e.g., agency, division, office and/or staff)	Internal Control Existence (a)				Performance Effectiveness					Description/Comments (this column must be completed) description of controls, activities, formal policies, procedures, and practices that represent internal controls related to the IT process and whether alternative or compensating controls and plans and time frames exist for addressing deficiencies	Monitoring (this column must be completed) description of activities performed to ensure controls in place are working
			Documented	Not Documented	No Control in Place	Not Applicable (b)	Excellent	Very Good	Satisfactory	Ineffective/Inefficient	Not Applicable		
covering in-house and contract developed software?													
Issue-Specific Policies													
Are measures in place to ensure that issue specific policies are established to document management decisions regarding certain activities, applications, systems, or technologies?	PO 6.10												
Communication of IT Security Awareness													
Are there periodic security and internal control awareness training programs in place?	PO 6.11												
Conclusion for this Section (Include All Weaknesses Identified)													
Personnel													
Objective: To acquire and maintain a motivated and competent workforce and maximize personnel contributions to the IT process.													
Potential/Likely Risks: There are not sound, fair, and transparent personnel management practices to recruit, compensate, train, appraise, promote, and dismiss staff.													
Personnel Training													
Are employees provided with orientation upon hiring and with on-going training to maintain their knowledge, skills, abilities, and security awareness to the level required to perform effectively?	PO 7.4												
Cross-Training or Staff Back-Up													
Is sufficient cross training or backup of identified key personnel provided to address unavailability?	PO 7.5												
Personnel Clearance Procedures													
Does agency and IT management ensure their personnel are subject to security clearances before they are hired, transferred, or promoted?	PO 7.6												
Job Change and Termination													
Are appropriate and timely actions taken regarding job terminations or job changes so internal controls and security are not impaired?	PO 7.8												
Conclusion for this Section (Include All Weaknesses Identified)													
External Requirements													

(a) When possible, obtain applicable documentation and/or flowcharts for your future needs/requirements.

(b) Please explain in the Description/Comments Column

(1)	(2)	(3)	(4)				(5)					(6)	(7)
Optimal Internal Controls	COBIT reference	Agency, Division/Office and Staff (non-DIT) responsible for IT process and related controls identify the activity and business owner responsible for each IT process (e.g., agency, division, office and/or staff)	Internal Control Existence (a)				Performance Effectiveness					Description/Comments (this column must be completed) description of controls, activities, formal policies, procedures, and practices that represent internal controls related to the IT process and whether alternative or compensating controls and plans and time frames exist for addressing deficiencies	Monitoring (this column must be completed) description of activities performed to ensure controls in place are working
			Documented	Not Documented	No Control in Place	Not Applicable (b)	Excellent	Very Good	Satisfactory	Ineffective/Inefficient	Not Applicable		
Objective: To meet legal, regulatory, and contractual obligations.													
Potential/Likely Risks: The organization does not identify and analyze external requirements for their IT impact, and take appropriate measures to comply with them.													
External Requirements Review													
Are procedures in place to coordinate activities related to performing a comprehensive and ongoing review of external requirements?	PO 8.1												
Practices and Procedures for Complying with External Requirements													
Do organizational practices ensure that appropriate corrective actions are taken on a timely basis to guarantee compliance with external requirements?	PO 8.2												
Safety and Ergonomic Compliance													
Does management ensure compliance with safety and ergonomic standards in the working environment of IT users and personnel?	PO 8.3												
Privacy, Intellectual Property and Data Flow													
Does management ensure compliance with privacy, intellectual property, transborder data flow, and cryptographic regulations?	PO 8.4												
Electronic Commerce													
Does management ensure that formal contracts are in place establishing agreement between trading partners on communication processes, and standards for transacting message security and storage?	PO 8.5												
Compliance with Insurance Contracts													
Does management ensure that insurance contract requirements are identified and continuously met?	PO 8.6												
Conclusion for this Section (Include All Weaknesses Identified)													
Risk Assessment													
Objective: Determine that controls over the IT process of assessing risks helps satisfy the business requirements of ensuring the achievement of objectives and responding to the provision of IT services.													
Potential/Likely Risks: The process of IT risk identification and impact analysis, and taking cost effective measures to mitigate risks, is not undertaken by the organization.													
Business Risk Assessment													
Has a systematic assessment framework been established which incorporates a regular assessment of the relevant information risks to the	PO 9.1												

(a) When possible, obtain applicable documentation and/or flowcharts for your future needs/requirements.

(b) Please explain in the Description/Comments Column

(1)	(2)	(3)	(4)				(5)					(6)	(7)
Optimal Internal Controls	COBIT reference	Agency, Division/Office and Staff (non-DIT) responsible for IT process and related controls identify the activity and business owner responsible for each IT process (e.g., agency, division, office and/or staff)	Internal Control Existence (a)				Performance Effectiveness					Description/Comments (this column must be completed) description of controls, activities, formal policies, procedures, and practices that represent internal controls related to the IT process and whether alternative or compensating controls and plans and time frames exist for addressing deficiencies	Monitoring (this column must be completed) description of activities performed to ensure controls in place are working
			Documented	Not Documented	No Control in Place	Not Applicable (b)	Excellent	Very Good	Satisfactory	Ineffective/Inefficient	Not Applicable		
achievement of business objectives and forms a basis for determining how the risks should be measured to an acceptable level?													
Risk Assessment Approach													
Has a general risk assessment approach been established which defines the scope and boundaries, the methodology to be adopted for risk assessments, the responsibilities, and the required skills?	PO 9.2												
Risk Identification													
Does the risk assessment approach focus on the examination of the essential elements of risk such as assets, threats, vulnerabilities, safeguards, consequences, and the likelihood of threat?	PO 9.3												
Risk Measurement													
Does the risk assessment approach ensure that analysis of risk identification information results in a quantitative and qualitative measurement of risk to which the examined area is exposed?	PO 9.4												
Risk Action Plan													
Does the risk assessment approach provide for the definition of a risk action plan to ensure threat cost-effective controls and security measures mitigate exposure to risks on a continuing basis?	PO 9.5												
Risk Acceptance													
Does the risk assessment process approach ensure the formal acceptance of the residual risk depending on risk identification and measurement, organizational policy, uncertainty incorporated in the risk assessment approach itself, and the cost effectiveness of implementing safeguards and controls?	PO 9.6												
Safeguard Selection													
Are controls analyzed to ensure the best (e.g. cost effective) control is in place?	PO 9.7												
Risk Assessment Commitment													
Does management encourage risk assessment as a tool to provide useful internal control information?	PO 9.8												
Conclusion for this Section (Include All Weaknesses Identified)													

(a) When possible, obtain applicable documentation and/or flowcharts for your future needs/requirements. (b) Please explain in the Description/Comments Column

(1)	(2)	(3)	(4)				(5)					(6)	(7)
Optimal Internal Controls	COBIT reference	Agency, Division/Office and Staff (non-DIT) responsible for IT process and related controls identify the activity and business owner responsible for each IT process (e.g., agency, division, office and/or staff)	Internal Control Existence (a)				Performance Effectiveness					Description/Comments (this column must be completed) description of controls, activities, formal policies, procedures, and practices that represent internal controls related to the IT process and whether alternative or compensating controls and plans and time frames exist for addressing deficiencies	Monitoring (this column must be completed) description of activities performed to ensure controls in place are working
			Documented	Not Documented	No Control in Place	Not Applicable (b)	Excellent	Very Good	Satisfactory	Ineffective/Inefficient	Not Applicable		
Project Management													
Objective: To set priorities and ensure the project is completed on time and within the budget.													
Potential/Likely Risks: The organization does not identify and prioritize projects in line with perations, and it does not adopt and apply sound project management techniques for each project undertaken.													
Project Management Framework													
Do project management processes exist for planning, organizing, monitoring, and controlling all aspects of the project?	PO 10.1												
User Department Participation in Project Initiation													
Are formal, documented plans in place to involve appropriate levels of users throughout the project (from requirements definition to sign-off)?	PO 10.2												
Project Team Membership and Responsibilities													
Do clearly defined, documented, and understood responsibilities, accountabilities, and authorities exist for each member of the project team?	PO 10.3												
Project Definition													
Are project specifications precisely defined?	PO 10.4												
Project Approval													
Does management make project decisions based on data and factual information?	PO 10.5												
Project Phase Approval													
Has an acceptance procedure been defined and documented (e.g., formal acceptance/approval of major phases)?	PO 10.6												
Project Master Plan **System Quality Assurance Plan**													
Does an approved project and quality plan exist? Has the project plan been prepared to allow for measuring and assessing objectives/deliverables?	PO 10.7 PO 10.8												
Planning of Assurance Methods													
Are assurance tasks performed to ensure that internal controls and security features meet the related requirements?	PO 10.9												
Formal Project Risk Management													
Is risk assessment performed for each project?	PO 10.10												

(a) When possible, obtain applicable documentation and/or flowcharts for your future needs/requirements.

(b) Please explain in the Description/Comments Column

(1)	(2)	(3)	(4)				(5)					(6)	(7)
Optimal Internal Controls	COBIT reference	Agency, Division/Office and Staff (non-DIT) responsible for IT process and related controls identify the activity and business owner responsible for each IT process (e.g., agency, division, office and/or staff)	Internal Control Existence (a)				Performance Effectiveness					Description/Comments (this column must be completed) description of controls, activities, formal policies, procedures, and practices that represent internal controls related to the IT process and whether alternative or compensating controls and plans and time frames exist for addressing deficiencies	Monitoring (this column must be completed) description of activities performed to ensure controls in place are working
			Documented	Not Documented	No Control in Place	Not Applicable (b)	Excellent	Very Good	Satisfactory	Ineffective/Inefficient	Not Applicable		
Test Plan													
Is a test plan developed? Does it include all aspects of the new system and adequate testing prior to implementation?	PO 10.11												
Training Plan													
Is a formal training plan developed?	PO 10.12												
Post-Implementation Review Plan													
At project closure, is a complete project review concluded (regardless of the reason for project closure) to determine if implementation met the original objectives?	PO 10.13												

Conclusion for this Section (Include All Weaknesses Identified)

Quality Management

Objective: To develop and communicate the quality improvement plan.

Potential/Likely Risks: The organization does not plan, implement, or maintain quality management standards and systems to provide for distinct development phases, clear deliverables, and explicit responsibilities.

General Quality Plan **Quality Assurance Approach**													
Does a quality improvement plan exist? Does it include a description of the quality assurance activities (e.g., reviews, audits, and inspections)?	PO 11.1 PO 11.2												
Coordination and Communication													
Is there a process in place to ensure close coordination and communication between customers of IT and system implementers?	PO 11.8												
Reports of Quality Assurance Reviews													
Are reports of quality assurance reviewers prepared and submitted to user and IT management?	PO 11.19												

Conclusion for this Section (Include All Weaknesses Identified)

Identification of Automated Solutions

Objective: To ensure an effective and efficient approach exists to satisfy the user requirements.

(a) When possible, obtain applicable documentation and/or flowcharts for your future needs/requirements.

(b) Please explain in the Description/Comments Column

(1)	(2)	(3)	(4)				(5)					(6)	(7)
Optimal Internal Controls	COBIT reference	Agency, Division/Office and Staff (non-DIT) responsible for IT process and related controls identify the activity and business owner responsible for each IT process (e.g., agency, division, office and/or staff)	Internal Control Existence (a)				Performance Effectiveness					Description/Comments (this column must be completed) description of controls, activities, formal policies, procedures, and practices that represent internal controls related to the IT process and whether alternative or compensating controls and plans and time frames exist for addressing deficiencies	Monitoring (this column must be completed) description of activities performed to ensure controls in place are working
			Documented	Not Documented	No Control in Place	Not Applicable (b)	Excellent	Very Good	Satisfactory	Ineffective/Inefficient	Not Applicable		
Potential/Likely Risks: The organization does not clearly identify and analyze alternative opportunities measured against user requirements.													
Definition of Information Requirements													
Are the business requirements clearly defined before a development, implementation, or modification project is approved?	AI 1.1												
Formation of Acquisition Strategy													
Are information systems acquisitions, development, and maintenance considered in the context of the organization's IT long and short range plans? Is there a software acquisition strategy plan defining whether the software will be acquired off-the-shelf, developed internally or through contract, or by enhancing existing hardware?	AI 1.3												
Third-Party Service Requirements													
Is there an evaluation of the requirements and specifications for a RFP when dealing with a third party service vendor?	AI 1.4												
Formulation of Alternative Courses of Action **Technological Feasibility Study** **Economic Feasibility Study**													
Is there an analysis of the alternative courses of action that will satisfy the business requirements established for a proposed new or modified system? Is there an examination of the technological feasibility of each alternative? Is there an analysis of the costs and benefits associated with each alternative being considered?	AI 1.2 AI 1.5 AI 1.6												
Information Architecture													
Does management ensure attention is paid to the enterprise data model while solutions are being identified and analyzed for future feasibility?	AI1.7												
Risk Analysis Report													
Is there an analysis of security threats, potential vulnerabilities and impacts, and the feasible security and internal control safeguards for reducing or eliminating risk?	AI 1.8												
Cost Effective Security Controls													
Are there mechanisms in place to ensure that the costs and benefits of security are examined in monetary and non-monetary terms to guarantee that	AI 1.9												

(a) When possible, obtain applicable documentation and/or flowcharts for your future needs/requirements. (b) Please explain in the Description/Comments Column

(1)	(2)	(3)	(4)				(5)					(6)	(7)
Optimal Internal Controls	COBIT reference	Agency, Division/Office and Staff (non-DIT) responsible for IT process and related controls identify the activity and business owner responsible for each IT process (e.g., agency, division, office and/or staff)	Internal Control Existence (a)				Performance Effectiveness					Description/Comments (this column must be completed) description of controls, activities, formal policies, procedures, and practices that represent internal controls related to the IT process and whether alternative or compensating controls and plans and time frames exist for addressing deficiencies	Monitoring (this column must be completed) description of activities performed to ensure controls in place are working
			Documented	Not Documented	No Control in Place	Not Applicable (b)	Excellent	Very Good	Satisfactory	Ineffective/Inefficient	Not Applicable		
the costs of controls do not exceed the benefits?													
Ergonomics													
Does management ensure that the information systems development, implementation, and change projects undertaken by the IT function is aware of the ergonomic issues associated with the introduction of automated solutions?	AI 1.11												
Selection of System Software													
Does management ensure that a standard procedure is adhered to by IT to identify all potential system software programs that will satisfy its operational requirements?	AI 1.12												
Procurement Control													
Does management develop and implement a central procurement approach describing a commons set of procedures and standards to be followed in the procurement of IT related hardware, software, and services? Are products tested and reviewed prior to their use, and in the case of outside vendors, prior to their financial settlement?	AI 1.13												
Software Product Acquisition													
Does software product acquisition follow set procurement procedures?	AI 1.14												
Third-Party Software Maintenance													
Does management require that for licensed software acquired from third party providers, the providers have appropriate procedures to validate, protect, and maintain the software product's integrity rights?	AI 1.15												
Contract Application Programming													
Is the procurement of contract programming services justified with a written request for services from IT?	AI 1.16												
Acceptance of Facilities													
Does management ensure that an acceptance plan for facilities is provided and agreed upon with the supplier and defines the acceptance procedures and criteria?	AI 1.17												
Acceptance of Technology													
Does management ensure that an acceptance plan for specific technology is agreed upon with the supplier and defines the acceptance procedures and	AI 1.18												

(a) When possible, obtain applicable documentation and/or flowcharts for your future needs/requirements. (b) Please explain in the Description/Comments Column

(1)	(2)	(3)	(4)				(5)					(6)	(7)
Optimal Internal Controls	COBIT reference	Agency, Division/Office and Staff (non-DIT) responsible for IT process and related controls identify the activity and business owner responsible for each IT process (e.g., agency, division, office and/or staff)	Internal Control Existence (a)				Performance Effectiveness					Description/Comments (this column must be completed) description of controls, activities, formal policies, procedures, and practices that represent internal controls related to the IT process and whether alternative or compensating controls and plans and time frames exist for addressing deficiencies	Monitoring (this column must be completed) description of activities performed to ensure controls in place are working
			Documented	Not Documented	No Control in Place	Not Applicable (b)	Excellent	Very Good	Satisfactory	Ineffective/Inefficient	Not Applicable		
criteria?													

Conclusion for this Section (Include All Weaknesses Identified)

Acquisition and Maintenance of Application Software													
Objective: To provide automated systems that effectively support the business function.													
Potential/Likely Risks: Specific statements of functional and operational requirements are not defined. A phased implementation does not identify clear deliverables.													
Design Methods													
Are appropriate procedures and techniques in conjunction with the system users' input, applied to create the design specifications for each new information system development project and do they verify the design specifications against the user requirements?	AI 2.1												
Major Changes to Existing Systems													
Does management ensure that in the event of major changes to the existing systems, a similar development process is observed, as is the case with the development of new systems?	AI 2.2												
Design Approval													
Are the design specifications for all information systems development and modification projects reviewed and approved by management, the affected user departments, and senior management, when appropriate?	AI 2.3												
File Requirements Definition and Documentation													
Is an appropriate procedure applied for defining and documenting the file format for each information system development or modification project?	AI 2.4												
Programming Specifications													
Are detailed written program specifications prepared for each information system development or modification project? Do they ensure that program specifications agree with system design specifications?	AI 2.5												
Source Data Collection Design													
Are adequate mechanisms for the collection and entry of data specified for each information system	AI 2.6												

(a) When possible, obtain applicable documentation and/or flowcharts for your future needs/requirements. (b) Please explain in the Description/Comments Column

(1)	(2)	(3)	(4)				(5)					(6)	(7)
Optimal Internal Controls	COBIT reference	Agency, Division/Office and Staff (non-DIT) responsible for IT process and related controls identify the activity and business owner responsible for each IT process (e.g., agency, division, office and/or staff)	Internal Control Existence (a)				Performance Effectiveness					Description/Comments (this column must be completed) description of controls, activities, formal policies, procedures, and practices that represent internal controls related to the IT process and whether alternative or compensating controls and plans and time frames exist for addressing deficiencies	Monitoring (this column must be completed) description of activities performed to ensure controls in place are working
			Documented	Not Documented	No Control in Place	Not Applicable (b)	Excellent	Very Good	Satisfactory	Ineffective/Inefficient	Not Applicable		
development or modification project?													
Input Requirements Definition and Documentation													
Do adequate mechanisms exist for defining and documenting the input requirements for each information system development or modification project?	AI 2.7												
Definition of Interfaces													
Are all external and internal interfaces properly specified, designed, and documented?	AI 2.8												
User-Machine Interface													
Does the system provide for the development of an interface between the user and machine, which is easy to use and self-documenting (by the means of on-line help functions0?	AI 2.9												
Processing Requirements Definitions and Documentation													
Do adequate mechanisms exist for defining and documenting the processing requirements for each information system development or modification project?	AI 2.10												
Output Requirements Definition and Documentation													
Do adequate mechanisms exist for defining and documenting the output requirements for each information system development or modification project?	AI 2.11												
Controllability													
Do adequate mechanisms exist for assuring the internal control and security requirements for each information system development or modification project?	AI 2.12												
Availability as a Key Design Factor													
Is availability considered in the design process for new or modified systems at the earliest stage possible?	AI 2.13												
IT Integrity Provisions in Application Program Software													
Are procedures established to ensure that application programs contain provisions that routinely verify the tasks performed by the software to help ensure data integrity through rollback or other means?	AI 2.14												

(a) When possible, obtain applicable documentation and/or flowcharts for your future needs/requirements. (b) Please explain in the Description/Comments Column

(1)	(2)	(3)	(4)				(5)					(6)	(7)
Optimal Internal Controls	COBIT reference	Agency, Division/Office and Staff (non-DIT) responsible for IT process and related controls identify the activity and business owner responsible for each IT process (e.g., agency, division, office and/or staff)	Internal Control Existence (a)				Performance Effectiveness					Description/Comments (this column must be completed) description of controls, activities, formal policies, procedures, and practices that represent internal controls related to the IT process and whether alternative or compensating controls and plans and time frames exist for addressing deficiencies	Monitoring (this column must be completed) description of activities performed to ensure controls in place are working
			Documented	Not Documented	No Control in Place	Not Applicable (b)	Excellent	Very Good	Satisfactory	Ineffective/Inefficient	Not Applicable		
Application Software Testing													
Are unit testing, application testing, integration testing, and load and stress testing performed according to the project test plan and established testing methods?	AI 2.15												
Reassessment of System Design													
Is the system design reassessed whenever significant and/or logical discrepancies occur during system development or maintenance?	AI 2.17												

Conclusion for this Section (Include All Weaknesses Identified)

Develop and Maintain Procedures													
Objective: To ensure the proper use of the applications and the technological solutions put in place.													
Potential/Likely Risks: There is not a structured approach to the development of user and operations procedures manuals, service requirements, and training manuals.													
Operational Requirements and Service Levels													
Are timely definitions of operational requirements and services levels ensured?	AI 4.1												
Training Materials													
Are adequate training materials developed as part of every information system development, implementation, or modification project?	AI 4.4												

Conclusion for this Section (Include All Weaknesses Identified)

Install and Accredit Systems													
Objective: Determine that the SDLC incorporates a process related to the installation and accreditation of the information systems.													
Potential/Likely Risks: There is not a well-formalized installation migration, conversion, and acceptance plan.													
Training													
Is the staff of the affected user groups trained as part of every information systems development, implementation, or modification project?	AI 5.1												
Implementation Plan													
Is an implementation plan prepared, reviewed, and approved by relevant parties and used to measure	AI 5.3												

(a) When possible, obtain applicable documentation and/or flowcharts for your future needs/requirements.

(b) Please explain in the Description/Comments Column

(1)	(2)	(3)	(4)				(5)					(6)	(7)
Optimal Internal Controls	COBIT reference	Agency, Division/Office and Staff (non-DIT) responsible for IT process and related controls identify the activity and business owner responsible for each IT process (e.g., agency, division, office and/or staff)	Internal Control Existence (a)				Performance Effectiveness					Description/Comments (this column must be completed) description of controls, activities, formal policies, procedures, and practices that represent internal controls related to the IT process and whether alternative or compensating controls and plans and time frames exist for addressing deficiencies	Monitoring (this column must be completed) description of activities performed to ensure controls in place are working
			Documented	Not Documented	No Control in Place	Not Applicable (b)	Excellent	Very Good	Satisfactory	Ineffective/Inefficient	Not Applicable		
progress?													
Data Conversion													
Is a data conversion plan prepared, defining the methods of collecting and verifying data to be converted and identifying any errors found during the conversion?	AI 5.5												
Testing Strategies and Plans													
Are testing strategies and plans prepared and signed off by the system owner and IT management?	AI 5.6												
Testing of Changes													
Does management ensure that changes are tested in accordance with the impact and resources assessment in a separate test environment by an independent (from builders) test group before regular use begins?	AI 5.7												
Parallel/Pilot Testing Criteria and Performance													
Are procedures in place to ensure that parallel or pilot testing is performed in accordance with a pre-established plan and that the testing process is specified in advance?	AI 5.8												
Final Acceptance Test **Security Testing and Accreditation** **Operational Test** **Evaluation of Meeting User Requirements** **Management's Post-Implementation Review**													
Are users involved during application development, in the testing of changes, final acceptance testing, security testing accreditation, operational testing, and is a post implementation review completed?	AI 5.9 AI 5.10 AI 5.11 AI 5.13 AI 5.14												
Promotion to Production													
Did management define and implement formal procedures to control the hand over of the system from the development to testing operations? Does management require the new system owner's authorization? Is the new system required to be operated through daily, monthly, and quarterly cycles prior to the old system being discontinued?	AI 5.12												

(a) When possible, obtain applicable documentation and/or flowcharts for your future needs/requirements.

(b) Please explain in the Description/Comments Column

(1)	(2)	(3)	(4)				(5)					(6)	(7)
Optimal Internal Controls	COBIT reference	Agency, Division/Office and Staff (non-DIT) responsible for IT process and related controls identify the activity and business owner responsible for each IT process (e.g., agency, division, office and/or staff)	Internal Control Existence (a)				Performance Effectiveness					Description/Comments (this column must be completed) description of controls, activities, formal policies, procedures, and practices that represent internal controls related to the IT process and whether alternative or compensating controls and plans and time frames exist for addressing deficiencies	Monitoring (this column must be completed) description of activities performed to ensure controls in place are working
			Documented	Not Documented	No Control in Place	Not Applicable (b)	Excellent	Very Good	Satisfactory	Ineffective/Inefficient	Not Applicable		
Conclusion for this Section (Include All Weaknesses Identified)													
Service Level Agreements													
Objective: Determine that formal service level agreements, which define the performance criteria against which the quantity and quality of service will be measured, have been established.													
Potential/Likely Risks: There are not service level agreements which formalize the performance criteria against which the quantity and quality of service will be measured.													
Service Level Agreement Framework **Aspects of Service Level Agreements**													
Is there documentation that a service level agreement is in place between the information systems function (e.g., DIT, etc.) and the user (e.g., business owner) that describes the service level in qualitative and quantitative terms?	DS 1.1 DS 1.2												
Service Level Agreement Framework													
Have formal service level agreements been established and documented with third party providers, if applicable?	DS 1.1												
Performance Procedures													
Are there procedures in place which ensure that the manner of and responsibilities for performance governing relations (e.g. non-disclosure agreements) between all parties involved are established, coordinated, maintained, and communicated to all affected?	DS 1.3												
Monitoring and Reporting **Review of Service Level Agreements and Contracts**													
Is there a periodic review of service level agreements and reporting of project process?	DS 1.4 DS 1.5												
Chargeable Items													
Do provisions of the service level agreement include provisions for chargeable items to make trade offs possible on service levels versus costs?	DS 1.6												
Service Improvement Program													
Has a service improvement plan been implemented for pursuing cost justified improvements to the service level?	DS 1.7												
Conclusion for this Section (Include All Weaknesses Identified)													

(a) When possible, obtain applicable documentation and/or flowcharts for your future needs/requirements. (b) Please explain in the Description/Comments Column

(1)	(2)	(3)	(4)				(5)					(6)	(7)
Optimal Internal Controls	COBIT reference	Agency, Division/Office and Staff (non-DIT) responsible for IT process and related controls identify the activity and business owner responsible for each IT process (e.g., agency, division, office and/or staff)	Internal Control Existence (a)				Performance Effectiveness					Description/Comments (this column must be completed) description of controls, activities, formal policies, procedures, and practices that represent internal controls related to the IT process and whether alternative or compensating controls and plans and time frames exist for addressing deficiencies	Monitoring (this column must be completed) description of activities performed to ensure controls in place are working
			Documented	Not Documented	No Control in Place	Not Applicable (b)	Excellent	Very Good	Satisfactory	Ineffective/Inefficient	Not Applicable		
Third Party Services													
Objective: To determine that the roles and responsibilities of third parties are clearly defined, adhered to, and continue to satisfy requirements.													
Potential/Likely Risks: There are not control measures aimed at the review and monitoring of existing agreements and procedures for their effectiveness and compliance with organizational policy.													
Supplier Interfaces													
Does management ensure that all third party providers' services are properly identified and that the technical and organizational interfaces with suppliers are documented?	DS 2.1												
Third-Party Contracts													
Does management ensure a formal contract with the third is defined and agreed upon before the work starts?	DS 2.3												
Third-Party Qualifications													
Does management ensure that potential third parties are qualified to deliver the required service?	DS 2.4												
Outsourcing Contracts **Continuity of Services**													
Are there procedures that ensure that the contract between the facilities management provider and the organization is based on required processing levels, security, monitoring, continuity requirements, and other stipulations as appropriate?	DS 2.5 DS 2.6												
Security Relationships													
Does management ensure that security agreements are identified and explicitly stated and adhered to?	DS 2.7												
Monitoring **Owner Relationships**													
Is there a process for monitoring the third party service delivery to ensure compliance with the contract terms?	DS 2.8 DS 2.2												

Conclusion for this Section (Include All Weaknesses Identified)

Continuous Service
Objective: To ensure IT services are available and with a minimum business impact in the event of a major disruption.

(a) When possible, obtain applicable documentation and/or flowcharts for your future needs/requirements. (b) Please explain in the Description/Comments Column

(1)	(2)	(3)	(4)				(5)					(6)	(7)
Optimal Internal Controls	COBIT reference	Agency, Division/Office and Staff (non-DIT) responsible for IT process and related controls identify the activity and business owner responsible for each IT process (e.g., agency, division, office and/or staff)	Internal Control Existence (a)				Performance Effectiveness					Description/Comments (this column must be completed) description of controls, activities, formal policies, procedures, and practices that represent internal controls related to the IT process and whether alternative or compensating controls and plans and time frames exist for addressing deficiencies	Monitoring (this column must be completed) description of activities performed to ensure controls in place are working
			Documented	Not Documented	No Control in Place	Not Applicable (b)	Excellent	Very Good	Satisfactory	Ineffective/Inefficient	Not Applicable		
Potential/Likely Risks: The operational and IT continuity plan is not in line with the overall business continuity plan and its related business requirements.													
IT Continuity Framework **IT Continuity Plan Strategy and Philosophy** **IT Continuity Plan Contents** **Minimizing IT Continuity Requirements**													
Has the organization documented and implemented an adequate business continuity plan/disaster recovery plan?	DS 4.1 DS 4.2 DS 4.3 DS 4.4												
Maintaining the IT Continuity Plan													
Has management established procedures to ensure the business continuity plan/disaster recovery plan is up-to-date and reflects the actual business environment?	DS 4.5												
Testing the IT Continuity Plan													
Does management assess the continuity plan on a regular basis or when there are major changes to the business or IT structure?	DS 4.6												
IT Continuity Plan Training													
Does the disaster recovery methodology ensure all concerned parties receive regular training for procedures to be followed in case of an emergency?	DS 4.7												
IT Continuity Plan Distribution													
Have adequate backup, restart and recovery procedures been documented for this application and does the computer operations staff maintain a copy?	DS 4.8												
User Department Alternative Processing Back-Up Procedures													
Has the organization identified critical systems and sensitive data that requires backup?	DS 4.9												
Critical IT Resources **Back-Up Site and Hardware**													
Do user departments establish alternative processing procedures that will be used until the system is fully functional again? Do the backup procedures address frequency and retention of critical data and system files, backup media, periodic testing, restoration of backup media, and alternatives regarding the back-up site and hardware?	DS 4.10 DS 4.11												

(a) When possible, obtain applicable documentation and/or flowcharts for your future needs/requirements. (b) Please explain in the Description/Comments Column

(1)	(2)	(3)	(4)				(5)					(6)	(7)
Optimal Internal Controls	COBIT reference	Agency, Division/Office and Staff (non-DIT) responsible for IT process and related controls identify the activity and business owner responsible for each IT process (e.g., agency, division, office and/or staff)	Internal Control Existence (a)				Performance Effectiveness					Description/Comments (this column must be completed) description of controls, activities, formal policies, procedures, and practices that represent internal controls related to the IT process and whether alternative or compensating controls and plans and time frames exist for addressing deficiencies	Monitoring (this column must be completed) description of activities performed to ensure controls in place are working
			Documented	Not Documented	No Control in Place	Not Applicable (b)	Excellent	Very Good	Satisfactory	Ineffective/Inefficient	Not Applicable		
Offsite Back-Up Storage													
Are copies of critical system files and programs and backup tapes stored at an off-site facility?	DS 4.12												
Are end user agency management and data owners aware of the retention periods for the various key application data files, and are these managers satisfied with the length of retention for critical and/or sensitive data and system files?	DS 4.12												
Do the retention period satisfy aency management reporting, IRS reporting, legal and business requirements, and internal accounting requirements?	DS 4.12												
Is the data stored on files, tapes, or other media checked periodically to ensure readability. integrity, and correctness?	DS 4.12												
Wrap-Up Procedures													
Has management established procedures for assessing the adequacy of the disaster recovery plan and making a necessary change to the plan after successful resumption of the IT function after a disaster?	DS 4.13												

Conclusion for this Section (Include All Weaknesses Identified)

Identify and Allocate Costs													
Objective: To ensure a correct awareness of the costs attributable to IT services.													
Potential/Likely Risks: The cost accounting system does not ensure that costs are recorded, calculated and allocated to the required level of detail and to the appropriate service offering.													
Chargeable Items													
Do the provisions of the service level agreement contain provisions that ensure chargeable items are identifiable, measurable, and predictable by users?	DS 6.1												

Conclusion for this Section (Include All Weaknesses Identified)

Education and Training
Objective: To ensure that users make effective use of the technology available.
Potential/Likely Risks: Staff are not trained to utilize the technology available to them.

(a) When possible, obtain applicable documentation and/or flowcharts for your future needs/requirements. (b) Please explain in the Description/Comments Column

(1)	(2)	(3)	(4)				(5)					(6)	(7)
Optimal Internal Controls	COBIT reference	Agency, Division/Office and Staff (non-DIT) responsible for IT process and related controls identify the activity and business owner responsible for each IT process (e.g., agency, division, office and/or staff)	Internal Control Existence (a)				Performance Effectiveness					Description/Comments (this column must be completed) description of controls, activities, formal policies, procedures, and practices that represent internal controls related to the IT process and whether alternative or compensating controls and plans and time frames exist for addressing deficiencies	Monitoring (this column must be completed) description of activities performed to ensure controls in place are working
			Documented	Not Documented	No Control in Place	Not Applicable (b)	Excellent	Very Good	Satisfactory	Ineffective/Inefficient	Not Applicable		
Identification of Training Needs													
Are procedures in place for identifying and documenting the training needs of all personnel using information services?	DS 7.1												
Training Organization													
Based on the identified training needs, have target groups been defined, trainers appointed, and training sessions organized in a timely manner or have alternative methods been investigated?	DS 7.2												
Security Principles and Awareness Training													
Are all personnel trained and educated in system security principles?	DS 7.3												

Conclusion for this Section (Include All Weaknesses Identified)

Assist and Advise Information Technology Customers													
Objective: To determine that the controls over the IT process of assisting and advising IT customers satisfies the business requirements and ensures that problems experienced by users are resolved.													
Potential/Likely Risks: There is no help desk to provide first line support and advice.													
Help Desk													
Has a help desk function been implemented and do the individuals responsible for performing this function closely interact with problem agency management personnel?	DS 8.1												
Registration of Customer Queries													
Are procedures in place to ensure that the help desk adequately registers all customer queries?	DS 8.2												
Customer Query Escalation													
Do help desk procedures ensure that customer queries, which cannot immediately be resolved, are appropriately escalated within the information services function?	DS 8.3												
Monitoring of Clearance													
Have procedures been established for timely monitoring of the clearance of customer queries? Are long-standing queries investigated and acted upon?	DS 8.4												

(a) When possible, obtain applicable documentation and/or flowcharts for your future needs/requirements.

(b) Please explain in the Description/Comments Column

(1)	(2)	(3)	(4)				(5)					(6)	(7)
Optimal Internal Controls	COBIT reference	Agency, Division/Office and Staff (non-DIT) responsible for IT process and related controls identify the activity and business owner responsible for each IT process (e.g., agency, division, office and/or staff)	Internal Control Existence (a)				Performance Effectiveness					Description/Comments (this column must be completed) description of controls, activities, formal policies, procedures, and practices that represent internal controls related to the IT process and whether alternative or compensating controls and plans and time frames exist for addressing deficiencies	Monitoring (this column must be completed) description of activities performed to ensure controls in place are working
			Documented	Not Documented	No Control in Place	Not Applicable (b)	Excellent	Very Good	Satisfactory	Ineffective/Inefficient	Not Applicable		
Trend Analysis and Reporting													
Are there procedures in place that ensure adequate reporting with regard to customer queries and resolution, response times, and trend identification?	DS 8.5												
Conclusion for this Section (Include All Weaknesses Identified)													
Storage, Retrieval, and Recovery													
Objective: To determine that controls over file handling, file access, and backup and recovery are affective to ensure the completeness and accuracy of data during the process of data storage and retrieval.													
Potential/Likely Risks: There is not an effective combination of application and general controls over the IT operations.													
Media Library Management System													
Have procedures been established to ensure that the contents of its media library containing data are inventoried systematically, that any discrepancies disclosed by a physical inventory are remedied in a timely fashion, and that measures are taken to maintain the integrity of magnetic media stored in the library?	DS 11.21												
Media Library Management Responsibilities													
Have housekeeping procedures been designed to protect media library contents established by IT management? Have standards been defined for the external identification of magnetic media and the control of its physical movement and the storage to support accountability? Have responsibilities for media (magnetic tape cartridge, disks, and diskettes) library management been assigned to specific members of the IT function?	DS 11.22												
Back-Up and Restoration													
Do back-up and recovery plans include a review of business requirements, as well as the development, implementation, testing, and documentation of the recovery plan?	DS 11.23												
Back-Up Jobs													
Are procedures in place to ensure back-ups are conducted in accordance with the defined back-up strategy, and the usability of the back-ups is regularly verified?	DS 11.24												

(a) When possible, obtain applicable documentation and/or flowcharts for your future needs/requirements. (b) Please explain in the Description/Comments Column

(1)	(2)	(3)	(4)				(5)					(6)	(7)
Optimal Internal Controls	COBIT reference	Agency, Division/Office and Staff (non-DIT) responsible for IT process and related controls identify the activity and business owner responsible for each IT process (e.g., agency, division, office and/or staff)	Internal Control Existence (a)				Performance Effectiveness					Description/Comments (this column must be completed) description of controls, activities, formal policies, procedures, and practices that represent internal controls related to the IT process and whether alternative or compensating controls and plans and time frames exist for addressing deficiencies	Monitoring (this column must be completed) description of activities performed to ensure controls in place are working
			Documented	Not Documented	No Control in Place	Not Applicable (b)	Excellent	Very Good	Satisfactory	Ineffective/Inefficient	Not Applicable		
Back-Up Storage													
Do back-up IT procedures for IT related media include the proper storage of the data files, software, and related documentation, both on site and off site? Are back-ups stored securely and the storage sites periodically reviewed regarding physical access security and the security of the data files and other items?	DS 11.25												
Archiving													
Do the archives meet legal and business requirements, and are they properly safeguarded and accounted for?	DS 11.26												
Continued Integrity of Stored Data													
Is the integrity and the correctness of the data kept on files and other media (e.g., electronic cards) periodically checked? Is specific attention paid to value tokes, reference files, and files containing privacy information?	DS 11.30												

Conclusion for this Section (Include All Weaknesses Identified)

Monitoring the Processes													
Objective: Determine that there is an adequate mechanism in place to ensure that key performance objectives set for the IT processes are being achieved.													
Potential/Likely Risks: Relevant performance indicators or reporting structures are not defined so deviations can be acted upon promptly.													
Collecting Monitoring Data													
For the IT and internal control processes, have relevant performance indicators (e.g., benchmarks) from both internal and external sources been defined and is data being collected for the creation of agency management information reports and exception reports regarding these indicators?	M 1.1												
Assessing Performance													
Are services delivered by the information services function measured (key performance indicators and/or critical success factors) by agency management and compared with target levels?	M 1.2												

(a) When possible, obtain applicable documentation and/or flowcharts for your future needs/requirements. (b) Please explain in the Description/Comments Column

(1)	(2)	(3)	(4)				(5)					(6)	(7)
Optimal Internal Controls	COBIT reference	Agency, Division/Office and Staff (non-DIT) responsible for IT process and related controls identify the activity and business owner responsible for each IT process (e.g., agency, division, office and/or staff)	Internal Control Existence (a)				Performance Effectiveness					Description/Comments (this column must be completed) description of controls, activities, formal policies, procedures, and practices that represent internal controls related to the IT process and whether alternative or compensating controls and plans and time frames exist for addressing deficiencies	Monitoring (this column must be completed) description of activities performed to ensure controls in place are working
			Documented	Not Documented	No Control in Place	Not Applicable (b)	Excellent	Very Good	Satisfactory	Ineffective/Inefficient	Not Applicable		
Assessing Customer Satisfaction													
Is customer satisfaction regarding the services delivered by the information services function measured at regular intervals to identify shortfalls and establish improvement objectives?	M 1.3												
Management Reporting													
Are agency management reports of the organization's progress toward the identified goals produced and is agency management periodically reviewing these reports?	M 1.4												

Conclusion for this Section (Include All Weaknesses Identified)

Assessing Internal Control Adequacy													
Objective: To ensure the achievement of the internal controls objectives set for the IT process.													
Potential/Likely Risks: There is not a commitment to monitor internal controls, assess their effectiveness, and report on them.													
Internal Control Monitoring													
Does agency management monitor the effectiveness of internal controls in the normal course of operations through management and supervisory activities, comparisons, reconciliations, and other routine actions?	M 2.1												
Timely Operation of Internal Controls													
Does the reliance on internal controls require that controls operate promptly to highlight errors and inconsistencies corrected before they impact production and delivery?	M 2.2												
Internal Control Level Reporting													
Does agency management report information on internal control levels and exceptions to the affected parties to ensure the continued effectiveness of its internal control system?	M 2.3												
Operational Security and Internal Control Assurance													
Are operational security and internal control assurance established with self-assessment or independent audit to examine whether or not the security and internal controls are operating according to the stated or implied security and	M 2.4												

(a) When possible, obtain applicable documentation and/or flowcharts for your future needs/requirements. (b) Please explain in the Description/Comments Column

(1)	(2)	(3)	(4)				(5)					(6)	(7)
Optimal Internal Controls	COBIT reference	Agency, Division/Office and Staff (non-DIT) responsible for IT process and related controls identify the activity and business owner responsible for each IT process (e.g., agency, division, office and/or staff)	Internal Control Existence (a)				Performance Effectiveness					Description/Comments (this column must be completed) description of controls, activities, formal policies, procedures, and practices that represent internal controls related to the IT process and whether alternative or compensating controls and plans and time frames exist for addressing deficiencies	Monitoring (this column must be completed) description of activities performed to ensure controls in place are working
			Documented	Not Documented	No Control in Place	Not Applicable (b)	Excellent	Very Good	Satisfactory	Ineffective/Inefficient	Not Applicable		
internal requirements?													

Conclusion for this Section (Include All Weaknesses Identified)

Obtain Independent Assurance													
Objective: Determine that there is a process in place for obtaining independent assurance.													
Potential/Likely Risks: Independent assurance reviews are not carried out at regular intervals.													
Independent Security and Internal Control Certification/Accreditation of IT Services													
Has independent certification/accreditation of security and internal controls been obtained prior to implementing critical new IT services and is re-certification/re-accreditation don a routine cycle after implementation?	M 3.1												
Independent Security and Internal Control Certification/Accreditation of Third-Party Service Providers													
Has independent certification/accreditation of security and internal controls been obtained prior to IT service providers and is re-certification/ re-accreditation done on a routine cycle?	M 3.2												
Independent Effectiveness Evaluation of IT Services													
Is there a regular, independent review of the effectiveness of IT services?	M 3.3												
Independent Effectiveness Evaluation of Third-Party Service Providers													
Is there a regular independent review of the effectiveness of the IT providers?	M 3.4												
Independent Assurance of Compliance with Laws and Regulatory Requirements and Contractual Commitments													
Is there a regular review of application systems to ensure compliance with external policies and standards (e.g., SAS 70, HIPPA, federal regulations, state regulations, local laws, customs worldwide, etc.)?	M 3.5												
Is there a regular review of application systems to ensure compliance with internal policies and standards?													
Independent Assurance of Compliance with Laws and Regulatory Requirements and Contractual Commitments by Third-Party Service Providers													
Has independent assurance of third party service providers' compliance with legal and regulatory requirements and contractual commitments been obtained and is this performed on a routine cycle?	M 3.6												

(a) When possible, obtain applicable documentation and/or flowcharts for your future needs/requirements. (b) Please explain in the Description/Comments Column

(1)	(2)	(3)	(4)				(5)					(6)	(7)
Optimal Internal Controls	COBIT reference	Agency, Division/Office and Staff (non-DIT) responsible for IT process and related controls identify the activity and business owner responsible for each IT process (e.g., agency, division, office and/or staff)	Internal Control Existence (a)				Performance Effectiveness					Description/Comments (this column must be completed) description of controls, activities, formal policies, procedures, and practices that represent internal controls related to the IT process and whether alternative or compensating controls and plans and time frames exist for addressing deficiencies	Monitoring (this column must be completed) description of activities performed to ensure controls in place are working
			Documented	Not Documented	No Control in Place	Not Applicable (b)	Excellent	Very Good	Satisfactory	Ineffective/Inefficient	Not Applicable		
Competence of Independent Assurance Function													
Does agency management ensure that the independent assurance function possesses the technical competence, skills, and knowledge necessary to perform such reviews in an effective, efficient, and economical manner?	M 3.7												
Proactive Audit Involvement													
Does agency and IT management seek audit involvement in a proactive manner before finalizing IT service solutions?	M 3.8												

Conclusion for this Section (Include All Weaknesses Identified)

Provide for an Independent Audit													
Objective: Independent audits are carried out at regular intervals.													
Potential/Likely Risks: Independent audits are not conducted on a routine basis.													
Audit Charter													
Has agency management established a charter for the audit function and does the document outline the responsibility, authority, and accountability of the audit function?	M 4.1												
Independence													
Is the auditor independent form the auditee in attitude and appearance (actual and perceived)?	M 4.2												
Professional Ethics and Standards													
Does the audit function ensure adherence to applicable codes of professional ethics and auditing standards and is due professional care exercised in all aspects of the audit work, including the observance of applicable audit and information technology standards?	M 4.3												
Competence													
Are the auditors responsible for the review of the organization's information services function activities technically competent and do they collectively possess the skills and knowledge necessary to perform such reviews in an effective, efficient, and economic manner?	M 4.4												

(a) When possible, obtain applicable documentation and/or flowcharts for your future needs/requirements. (b) Please explain in the Description/Comments Column

(1)	(2)	(3)	(4)				(5)					(6)	(7)
Optimal Internal Controls	COBIT reference	Agency, Division/Office and Staff (non-DIT) responsible for IT process and related controls identify the activity and business owner responsible for each IT process (e.g., agency, division, office and/or staff)	Internal Control Existence (a)				Performance Effectiveness					Description/Comments (this column must be completed) description of controls, activities, formal policies, procedures, and practices that represent internal controls related to the IT process and whether alternative or compensating controls and plans and time frames exist for addressing deficiencies	Monitoring (this column must be completed) description of activities performed to ensure controls in place are working
			Documented	Not Documented	No Control in Place	Not Applicable (b)	Excellent	Very Good	Satisfactory	Ineffective/Inefficient	Not Applicable		
Planning													
Has a plan been established to ensure that regular and independent audits are obtained regarding the effectiveness, efficiency, and economy of security and internal control procedures, and agency management's ability to control information services function activities?	M 4.5												
Performance of Audit Work													
Are audits appropriately supervised to provide assurances that audit objectives are achieved and applicable to professional auditing standards are met?	M 4.6												
Reporting													
Does the organization's audit function provide a report, in an appropriate form, to intended recipients upon the completion of the audit work?	M 4.7												
Follow-Up Activities													
Has resolution of previous audit comments, findings, conclusions, and recommendations been addressed by agency management and implemented in a timely manner?	M 4.8												

Conclusion for this Section (Include All Weaknesses Identified)

Overall Conclusion of Strengths and Weaknesses

As (job title) of the (office) of (department), I am cognizant of the importance of internal controls. I have taken necessary measures to ensure that the evaluation of the internal control structure has been conducted in a reasonable and prudent manner, in accordance with the General Framework for the Evaluation of Internal Controls, issued by the Department of Management and Budget, Office of Financial Management, in consultation with the Auditor General.

Objectives of the internal control structure are to provide reasonable assurance that measures are being used to safeguard assets, check the accuracy and reliability of accounting data, promote operational efficiency, and encourage adherence to prescribed managerial policies. The concept of reasonable assurance recognizes that the cost of internal control should not exceed benefits to be derived therefrom, and that benefits consist of reductions in risks of failing to achieve stated objectives.

(a) When possible, obtain applicable documentation and/or flowcharts for your future needs/requirements.

(b) Please explain in the Description/Comments Column

(1)	(2)	(3)	(4)				(5)					(6)	(7)
Optimal Internal Controls	COBIT reference	Agency, Division/Office and Staff (non-DIT) responsible for IT process and related controls identify the activity and business owner responsible for each IT process (e.g., agency, division, office and/or staff)	Internal Control Existence (a)				Performance Effectiveness					Description/Comments (this column must be completed) description of controls, activities, formal policies, procedures, and practices that represent internal controls related to the IT process and whether alternative or compensating controls and plans and time frames exist for addressing deficiencies	Monitoring (this column must be completed) description of activities performed to ensure controls in place are working
			Documented	Not Documented	No Control in Place	Not Applicable (b)	Excellent	Very Good	Satisfactory	Ineffective/Inefficient	Not Applicable		

The results of the evaluation indicate that the internal control structure in effect for the two-year period ended September 30, 2004, complies with the requirement to provide reasonable assurance that the aforementioned objectives were achieved, unless otherwise indicated below.

Material Weaknesses Identified: _____ Yes _____ No (If yes, attach to this letter a list of material weaknesses identified.)

Activity Level Manager Signature

Date

(a) When possible, obtain applicable documentation and/or flowcharts for your future needs/requirements.

(b) Please explain in the Description/Comments Column